УДК 621.391:336.71

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ЧАСІ

Євген Осадчий, Вячеслав Курченко, Дмитро Гриценко, Олександр Осадчий

Міжнародний науково-навчальний центр ЮНЕСКО/МПІ інформаційних технологій та систем НАН і Міносвіти та науки України

Анотація: **Пропонується нетрадиційний підхід до вирішення сучасних проблем захисту інформації при її транспортуванні з використанням таймерних методів та засобів перетворення. В доступному вигляді обґрунтовуються алгоритмічні та технічні аспекти цього напрямку та їх значення для сучасних інформаційних технологій.**

Summary: **Untraditional handling of modern problems of information security during its transmission using timer methods and means of transformation has been offered. Has been given grounds for algoritmic and technical aspects of such approach and its significance for modern information technologies.**

Ключові слова: **Таймерні методи та засоби, захист інформації**

I Вступ

Сучасний рівень розвитку обчислювальної техніки, засобів зв'язку та інформаційних технологій створили умови для розповсюдження глобальних мереж та засобів комунікації, що потребує відповідного правового, нормативного та метрологічного забезпечення захисту інформації. Підтвердженням цього є рішення про організацію в рамках ISO/IEC Joint Technical Committee нових підкомітетів і в тому числі IT Security techniques. Разом з тим, інтенсивний розвиток сучасної комп'ютерної техніки та засобів комунікацій, базований виключно на двійковому кодуванні та Фон-Неймановській архітектурі ЕОМ, наближається до своєї фізичної межі. Наприклад, вже практично досягнено теоретичного обмеження в алгоритмічних методах знакового стиснення інформації. Не дивлячись на те, що досягнено великої швидкодії обробки та щільності запису інформації в електронно-обчислювальних машинах (ЕОМ), прогнозована динаміка подальшого збільшення цих параметрів значно відстає від тієї, що існувала на попередніх етапах еволюції розвитку обчислювальних пристроїв, машин та систем. Та особливо вражаючою є невідповідність між швидкодією обробки та транспортуванням інформації по каналам зв'язку. І об'єктивно, ця невідповідність буде поглиблюватись. Це пояснюється існуючими теоретичними і практичними обмеженнями розпаралелювання при транспортуванні навіть невеликих обсягів інформації. Вплив існуючих обмежень на покращення методів та засобів транспортування інформації значно посилюється вимогами забезпечення захисту інформації. У свою чергу, розповсюдження комп'ютерних технологій, розвиток систем комп'ютерних телекомунікацій та інтегрованих баз даних ще більше підвищили актуальність цих проблем. Тому, перш за все, обмежимось висвітленням можливостей їх вирішення шляхом використання нетрадиційних (таймерних) методів та засобів обробки інформації.

II Основна частина

Так склалося, що “таймерні” методи та засоби обробки інформації, тобто такі, що базуються на часових операційних (машинних) параметрах, до даного часу не отримали широкого визнання в інформаційних технологіях.

Перш ніж зупинитись на перспективах розвитку цих методів та засобів, наведемо короткий історичний екскурс. Як відомий приклад використання таймерного підходу до вирішення проблеми захисту каналу зв'язку, можна привести домовленість про виконання якихось дій сценарію в залежності від часу отримання умовного сигналу. Аналогічно вирішується проблема стиснення, тільки кожному часовому інтервалу ставиться у відповідність інформація або адреса її знаходження. Відносно сучасних проблем захисту інформації - є умова використання таймерного ключа перед введенням традиційного числового ключа доступу. Тобто, доступ на введення паролю для ідентифікації користувача інформаційних ресурсів дозволяється у визначений часовий інтервал. Першим таймерним засобом у цифровій комп'ютерній техніці слід вважати появу в її складі “таймеру”, який можна вважати своєрідним паралельним міні-процесором. Функціональні можливості таймеру обмежені, він виконує лише роль своєрідного будильника, але значення його важко переоцінити. Так звана “проблема 2000 року” похідна від недооцінення задач часового узгодження.

Основним елементом більшості сучасних систем захисту інформації від несанкціонованого доступу є криптографічне кодування, яке в свою чергу базується на відповідних алгоритмах. Але проблемою

криптоаналізу є лише час, а сучасна тенденція швидкого зростання продуктивності комп'ютерів та можливості організації паралельного рішення задач на багатопроцесорних комп'ютерах та комп'ютерах з'єднаних у мережу, різко знижує захищеність багатьох традиційних криптографічних алгоритмів. Так наприклад, доведено, що задача злому будь-якого криптографічного алгоритму завжди може бути зведена до рішення системи нелінійних булевих рівнянь. Тому рішення проблеми слід шукати не на алгоритмічному рівні, а на фізичному, тобто в засобах подання інформації.

Одним з найефективніших методів захисту інформації, що базується на іншому фізичному засобі представлення інформації, є таймерний метод. Операційним параметром в даному випадку є не струм або напруга (як у традиційній обчислювальній техніці), а час. В таких пристроях часозадаючими елементами служать аналогові, RL, RC кола і вони отримали назву таймерних обчислювальних приладів (ТОП). В цифрових ТОП використовуються лічильниково-регістрові структури.

В ТОП обробка, зберігання і передача інформації здійснюється у вигляді таймерних операндів. Кожен таймерний операнд являє собою кортеж часових інтервалів, тривалість яких має конкретні числові значення. Так, ціле невід'ємне число подається інтервалом часу

$$\tau = X/F_k, \qquad (1)$$

де F_k - частота елементарних квантуючих імпульсів, фіксуємих цифровим лічильником ТОП, що заповнюють кодуємий інтервал.

Збільшення швидкодії та підвищення точності ТОП в першу чергу пов'язане з необхідністю зменшення тривалості обробки. Але для того, щоб знизити ймовірність розшифрування інформації, доводиться використовувати великі часові інтервали при шифруванні. Чим більший інтервал, тим менша ймовірність розшифрування.

Наприклад: Маємо число для шифрування 1000, частота дискретизації передаючого та приймаючого пристроїв -1кГц. Отже, для наведення даної інформації потрібен інтервал одна секунда. Для спостерігача, який не знає частоти дискретизації передаючого та приймаючого пристроїв щоб розшифрувати закодовану інформацію необхідно перебрати всі можливі частоти дискретизації. При кожній спробі сторонньому спостерігачу доводиться чекати 1 секунду, що навіть при невеликій, з погляду теорії захисту інформації, кількості можливих варіантів підбору випливає в досить вагомі проміжки часу.

В загальному виді пристрій, який виконуватиме роль вимірювача часових інтервалів, можна представити у вигляді середовища з певним постійно заданим та рівномірним протягом сеансів прийому та передачі вповільненням часу. Фактично інтервал часу, що представляє певну частину інформації, зводиться до такого масштабу, щоб його можна було розпізнати відомими пристроями та представити у прийнятній формі (двійкова система). Лічильник, який виконує узгоджуючу функцію в такій моделі, може бути представлений у вигляді, зображеному на рисунку 1. При цьому, потік вхідної інформації (двійкової) спрямовується через "Вхідний перетворювач" на один з елементів у вигляді одиниці і кількох нулів, на виході середовища (в даному випадку лінійний ланцюг) отримуємо часовий інтервал. При отриманні вхідного часового інформаційного інтервалу він потрапляє у середовище, результатом перетворення інформації з якого є потік вихідної інформації.

Масштабування при такій реалізації можна задавати, регулюючи час затримки на вповільнюючих елементах, або, що простіше реалізується, введенням синхронізації елементів пам'яті.

У якості даного пристрою може бути використаний, наприклад, надшвидкісний N-розрядний лічильник для задання та вимірювання часових інтервалів. Особливістю такого лічильника є наявність в структурі значної кількості простих однотипних елементів. Кількість елементів експоненціально залежить від розрядності лічильника. Але сучасний рівень інтеграції цифрових схем дає можливість використовувати навіть громіздкі лічильники для підвищення швидкості і рівномірності відліку. Саме ці ознаки присутні в даному N-розрядному лічильнику.

Зсувний ланцюг з D тригерів, що лежить в основі N-розрядного лічильника, дає змогу зробити моментальний знімок часового інтервалу, або миттєво відтворити його. Така швидкодія дозволяє вирішити вищевказані проблеми таймерного кодування. При цьому не є обмеженням те, що час, потрібний для двійкового дешифрування, може бути відносно значним. Так, навіть за цим параметром, по наших розрахунках, до величини 32 розрядного двійкового числа такий лічильник не має конкурентів. Існує також безліч задач, коли не має істотного значення величина часу відтворення двійкового еквіваленту, а важливим є лише факт одержання та

відтворення моментального достовірного знімку часового інтервалу. Крім того, є алгоритмічні та технічні можливості розширення інтервалу 32 розрядного обмеження. Коли ж буде вирішено проблему переходу на нову таймерну елементну базу це обмеження взагалі не матиме суттєвого значення.

Покажемо, що використання N-розрядного лічильника в таймерному кодуванні дійсно дозволяє значно зменшити ймовірність злому при тих же розмірах часових інтервалів, або зменшити числові інтервали, збільшивши тим самим кількість інформації за одиницю часу, з тією ж ймовірністю злому.

Так при використанні звичайних лічильників

$$\tau_k = n\tau_T, \tag{2}$$

де τ_k-квант часу для переключення з *к*-1 на *к* двійковий код;

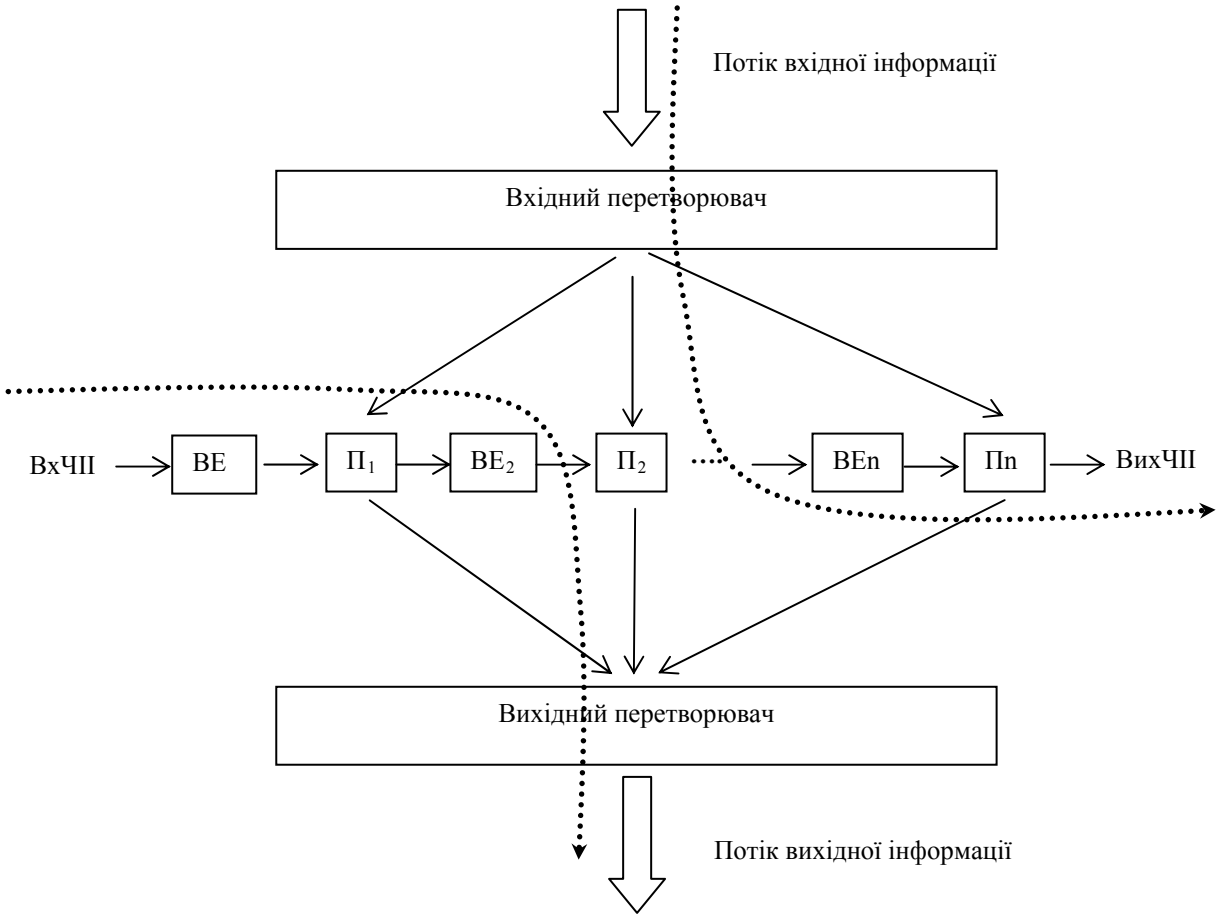
n-розрядність лічильника;

τ_T-квант часу для переключення одного розряду двійкового лічильника.

В разі N-розрядного лічильника

$$\tau_k = \tau_D, \tag{3}$$

де τ_D - квант часу для переключення одного розряду N-розрядного лічильника. Тут $\tau_T >> \tau_D$.



ВхЧІІ та ВихЧІІ – відповідно вхідний та вихідний часовий інформаційний інтервал;

ВЕі – вповільнюючий елемент; Пі – елемент пам’яті

Рисунок 1 – Схема загального вигляду узгоджуючого лічильника.

Важливим аргументом доцільності використання N-розрядного лічильника в таймерних методах захисту інформації є те, що при цьому спостерігатиметься зворотна по відношенню до криптографічних методів залежність надійності методу захисту від розвитку технологій у обчислювальній техніці.

Іншим аспектом вирішення проблеми захисту є можливість використання даного лічильника для забезпечення захисту інформації від руйнування та знищення. В цьому випадку дозволяється транспортування по каналам не множини двійкових кодів, що відповідають значенню повідомлення, а адекватної йому "одиничної" таймерної позначки. В зв'язку з обмеженням обсягів викладення результатів дослідження, розглянемо самий простий випадок, коли знімається обмеження на величину часу відтворення двійкового еквіваленту за допомогою шифратора.

Для розкриття значення цієї позначки приведемо зіставлення одного і того ж числа N в різних системах числення. У позиційній системі числення з основою p число N представляється у вигляді комбінації його ступенів з коефіцієнтом, що приймає значення від О до $p-1$, тобто у вигляді $a_k p^k + a_{k-1} p^{k-1} + ... + a_1 p_1 + a_0 p^0$, що еквівалентно скороченого запису $(a_k, a_{k-1}, ..., a_1, a_0)p$.

З приведеного виразу випливає, що в одному розряді системи числення з основою p можна відобразити $s = p$ символів. Відповідно, якщо є число *з* M символів, то необхідна кількість розрядів R, для запису цього числа в системі числення з основою p буде відповідати: $R = \frac{M}{p}$, так як $s = p$.

Уявімо далі, що є число N, яке відображене в системах числення з основою $p = (1,2,.., M)$, тоді в системі числення основою $p = 1$ задається M розрядів для запису числа N, а в системі з основою $p = M$ буде потрібний єдиний розряд. Звідси випливає, що в останньому випадку, для відображення числа N буде потрібний єдиний символ, що еквівалентно отриманню коду стиснення найбільшої компактності.

Відповідно, таким єдиним символом в нашому випадку є двійкова "1", яка розміщується в лінійному просторі інформаційного повідомлення. При цьому всі молодші розряди є двійковими "0", а кількість всіх розрядів повідомлення відповідає кількості чисел, отриманих двійковим додаванням "1", починаючи з "0" до абсолютної величини значення двійкового числа.

Наприклад, нехай інформаційним повідомленням є двійкове число 101. Тоді, його можна відобразити адекватним двійковим числом з одиничною позначкою як 00001. Таймерною ця позначка названа тому, що її двійкове шифрування в загальному вигляді відповідає таймерному перетворенню, тобто вона є лінійно залежною від часу.

Повідомлення, що представлене у такому вигляді легко можна захистити від руйнування та знищення, в тому числі з використанням існуючих алгоритмів, забезпечивши максимальний рівень захисту. В цьому випадку, N-розрядний лічильник в таймерному кодуванні використовується для двійкового дешифрування адекватного повідомлення у вигляді двійкового числа з одиничною позначкою.

Коли швидкодія N-розрядного лічильника настільки велика, що не забезпечує надійну роботу шифратора, то можна збільшити розмір одиничної позначки. Тобто ця позначка має бути у вигляді такої кількості "1", яка однозначно розпізнається шифратором. Можливі також інші альтернативні рішення.

III Висновок

Таким чином, транспортування інформації в таймерному вигляді дозволить підвищити ефективність її захисту, зберігання та передачі. Покращення перешкодозахищеності інформації підвищує безпеку її захисту від випадкових загроз безпеки. Тому, існують всі умови для широкого використання принципів таймерного кодування для розробки нових методів та засобів цифрового запису інформації з покращеними технічними характеристиками.